Security and Privacy Protection Action Plan ***DRAFT***
Executive Status Report
February 26, 2008

Requirements and Best Practices					
	Activity	**Owner**	**Assisting**	**Status**	**Comments**
1.	Strengthen policy governing the release of confidential CalPERS information	EXEO	GOVA HBB ISOF PAOF	Completed (8/17/07)	In addition to establishing business justification, all requests to use, access or release any data designated as confidential **must** be approved by a CalPERS official at or above the level of Assistant Executive Officer
2.	Establish a Privacy Protection and Security Task Force to provide guidance and oversight related to the handling and usage of confidential data	EXEO		Completed (9/4/07)	The Task Force, chaired by Gloria Moore-Andrews, Deputy Executive Officer - Operations, includes representatives from each business and support area.
3.	Analysis of AB 779	GOVA		Completed	AB 779 requires businesses and public agencies to safeguard sensitive information and would have codified the Payment Card Industry Data Security Standard and make entities responsible for security breaches financial liable. AB 779 was vetoed by the Governor
4.	Apply for CalPERS representation on the Health and Human Services Agency privacy and security Task Forces	HBB		Completed	
5.	Schedule Security and Privacy All Staff Forums and future training efforts to provide information to all staff	PAOF		Completed	Security and Privacy all staff forum scheduled for April 30, 2008

Electronic Storage, Access and Transfer					
	Activity	**Owner**	**Assisting**	**Status**	**Comments**
1.	Strengthen policy governing the release of confidential CalPERS information	EXEO		Completed (8/17/07)	In addition to establishing business justification, all requests to use, access or release any data designated as confidential **must** be approved by a CalPERS official at or above the level of Assistant Executive Officer
2.	Establish a Privacy Protection and Security Task Force to provide guidance and oversight related to the handling and usage of confidential data	EXEO		Completed (9/4/07)	The Task Force, chaired by Gloria Moore-Andrews, Deputy Executive Officer - Operations, includes representatives from each business and support area
3.	Update existing file transfer processes including, file exchanges with other State agencies such as SCO,DOF,STO, to comply with new policy requirements. Re-evaluate each instance of SSN usage to determine business need and eliminate wherever possible.				
	(a) Revise File layout and data transferred as part of 2009 Board Member election process	OSSD	MBSB ITSB	Planned	This task is on ITSB's list of efforts to be accomplished and will be completed before the system is required to support the Member At Large Election 2009.

	(b) Identify and report all existing production file transfers, including: descriptions of the data transferred; the purpose of the transfer; schedule (frequency) and destination (to whom and where).	ITSB		Completed (8/25/07)	
	(c) Bring all existing data transfer processes into compliance with new security policy requirements.	ISO	AESB MBSB HBSB INVO	In progress	The ISOF is coordinating with the respective divisions to review the information compiled and to determine business need. Estimated completion date is 5/1/08. A list of known file transfers has been distributed to AEOs, requesting prioritization of transfers by each Branch. ISOF is coordinating with each Branch to document file transfers and ensure that each is compliant with policies and practices. ISOF has requested contacts be identified within each Branch to facilitate this process. Over 250 data transfers have been identified. Currently, 14 or 6% are in compliance with new security policy requirements.
	(d) Determine business requirement for each file transfer that contains SSN; remove SSN where business justification does not exist.	ISO	AESB MBSB HBSB INVO	In progress	The ISOF is coordinating with the respective divisions to review the information compiled and to determine business need. Estimated completion date is 7/1/08

4.	Review standard Non-Disclosure Agreement (NDA) and ensure SEIA forms and contract template are consistent. Additionally, develop a plan for assessment of existing contracts for inclusion of standard Non-Disclosure Agreement. (a) Evaluate current standard NDA for compliance with laws, regulations, and CalPERS' Information Security Policies. (b) Ensure all existing SEIA NDA provisions is consistent with the standard NDA and amend existing SEIA, if necessary. (c) Validate contract template language, including attachments C or III, is consistent with standard NDA. (d) Develop a plan for enterprise-wide assessment of all contracts (including contracts developed by OSSD, or any other source), based on risk, to determine if contract amendments are necessary to include standard NDA either immediately or through contract amendment or renewal processes.	LEGO	OSSD HBB AESB ISO MBSB INVEST		<u>OSSD</u> All contracts that deal with Member information require a NDA, and some contracts, such as those dealing with PHI or ePHI, may require additional confidentiality and security provisions. All contracts currently include enforceable language for vendor breaches. The contract manager is responsible for monitoring and enforcing all provisions of the contract, including those provisions dealing with securing member information. Work in both program areas, ISO, and LEGO continues, however, and OSSD is involved in those efforts. As new requirements are defined, OSSD will incorporate them into CalPERS' contracts and procedures.

5.	(a) Enhance MyCalPERS (Phase 2) to include: • New identification criteria • Improved member registration and log-in processes • Enhanced system activity logging and monitoring	PAOF	MBSB ITSB		Estimated completion date is 5/4/08

6.	Research alternatives to using SSN as a key identifier. Review how CalPERS electronically receives, stores and utilizes members' SSNs and identify options for using a different, unique identifier or combination of data for CalPERS' internal systems				
	(a) Conduct technical review of all internal databases, process, screens and reports that contain SSNs	ITSB		In progress	Estimated effort is 4-6 weeks due to resource constraints. Estimates have been developed to minimize impact to PSR, MyCalPERS (Phase 2), Service Request Backlog and State Alternative Retirement Program Project. Estimated completion date is March 15, 2008 depending on workload.
	(b) Conduct business analysis to determine if the entire nine-digit SSN is required to determine if either: 1) an alternative unique identifier or 2) a combination of partial SSN coupled with other unique user information	ITSB	AESB HBSB MBSB INVO		Estimated effort is 12 - 14 weeks due to resource constraints. Estimates have been developed to minimize impact to PSR, MyCalPERS (Phase 2), Service Request Backlog, State Alternative Retirement Program and Open Enrollment
	(c) Develop recommendations depicting cost, timeline and impact analysis for each. Compile recommendations into "draft" FBR.	ITSB			
	(d) Present recommendations to Executive Staff for decision.	ITSB			

	(e) Finalize FBR based on Executive decision and submit as part of 2008/09 Budget process	ITSB			• First reading: 3/14 and 3/19 • Second reading: 4/18 and 4/23

Incoming Data					
	Activity	**Owner**	**Assisting**	**Status**	**Comments**
1.	Review incoming subpoenas and member request database to eliminate or block SSN.	LEGO	ASB ITSB	In process	
2.	Review mail room processes to ensure documents are handled w/ safeguards to protect private information	OSSD	ASB		
3.	Review DMC processes to ensure documents are handled w/ safeguards to protect private information	ASB			
4.	SSNs being faxed for member changes	MBSB			MBSB divisions to pick up the faxes and sort to processing areas at least twice per day.

5.	Establish Public Counter and physical space protocols in Regional Offices. Include postings and procedures along with method to monitor and report on variations.	MBSB	OSSD	Completed	OSSD will work with MBSB to develop physical space protocols in Regional offices.
6.	Establish Enterprise wide fax protocols and procedures	OSSD	OSSD HBB AESB ISO MBSB INVEST	In process	

Employee Privacy Issues					
	Activity	**Owner**	**Assisting**	**Status**	**Comments**
1.	Eliminate use of SSNs on TECs	ASB		Completed 3/1/08	
2.	Redact SSNs on all applications for employment	ASB		Completed 3/1/08	
3.	Eliminate use of SSNs on timesheets (STD 634)	ASB		Completed 3/1/08	
4.	Eliminate use of partial SSNs on Badge Request forms	ASB		In progress	
5.	Develop policy for conducting background checks on employees	ASB		In progress	
6.	Review policy to require SSNs for granting access to COMET and Smart Desk	ITSB		In progress	

Physical Security					
	Activity	**Owner**	**Assisting**	**Status**	**Comments**
1.	ITSB Testing Room	ASB/ITSB			
2.	Revise Badge Access procedures	ASB		Completed (see #4) above	
3.	Acquire the services of a consulting firm to conduct a “White Hat Hack” internal test	ISO		Completed	